UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,203	02/21/2001	Ariel Katz	1018.126US1	5124

23460 7590 09/20/2004

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 09/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

4

4

Office Action Summary	**Application No.** 09/681,203	**Applicant(s)** KATZ ET AL.	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 February 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 through 36 are presented for examination.

Drawings

2. The drawings are objected to under 37 CFR 1.83(b) because they are incomplete. 37 CFR 1.83(b) reads as follows:

> When the invention consists of an improvement on an old machine the drawing must when possible exhibit, in one or more views, the improved portion itself, disconnected from the old structure, and also in another view, so much only of the old structure as will suffice to show the connection of the invention therewith.

3. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled “Replacement Sheet” in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance. Parts of figures 1, 3, 5, and 6 have been cut off by the margins. Appropriate action is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 13 and 27 provides for the use of claims 1 and 14, respectively, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

6. Claims 13 and 27 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin, in view of U.S. Patent No. 6,393,568 to Ranger et al., hereinafter Ranger.

9. As per claim 1, Jardin teaches a method comprising:

receiving encrypted data from a client over an unsecure network in a first hop (Figures 1 [blocks 150], 3 [block 310], column 6, lines 1-13);

decrypting the encrypted data into decrypted data (Figure 3 [block 330], column 6, line 58 to column 7, line 5).

10. Jardin does not disclose performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result.

11. Ranger discloses performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network. Subsequently if the data did not contain a virus, Trojan horse, or any other malicious code, the decrypted data would be transferred to a server over a given network in the second hop. Jardin discloses transmitting the data to a server in at least figure 3, blocks 336 and 346, and column 7, lines 10-15 and lines 53-56. Ranger discloses transmitting uninfected data to the intended recipient after it has been determined that it does not contain malicious code in column 4, lines 38-53.

12. Regarding claims 2 and 15, Ranger teaches wherein performing the test relative to the decrypted data comprises examining the decrypted data for security purposes, such that the first result is the decrypted data not presenting the security risk (column 2, lines 24-56).

13. Regarding claim 3, Jardin teaches wherein sending the decrypted data to the origin server over the given network in the second hop comprises first encrypting the decrypted data into second encrypted data (Figure 3 [blocks 336]; column 7, lines 6-19).

14. Regarding claim 4, Jardin teaches wherein the given network is a secure network (column 6, lines 44-57).

15. With regards to claims 5 and 16, Jardin discloses wherein the servers are web servers thereby able to handle HTTP and IMAP.

16. Ranger discloses scanning e-mails thereby accounting for POP.

17. Regarding claim 6, neither Jardin nor Ranger teaches wherein the given network is one of the unsecure network and a second unsecure network. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the network comprise of a first and second network, since it has been held that merely rearranging the orientation of computers into a hierarchical fashion is a design choice typically made by the network engineer. See MPEP 2144.04; see *In re Japikse*, 181 F.2d 1019, 1023, 86 USPQ 70, 73 (CCPA 1950).

18. Regarding claim 7, Jardin teaches wherein the encrypted data is received from the client over the unsecure network in the first hop within a secure socket layer (SSL) session (column 4, lines 24-34).

19. Regarding claims 8 and 19, Jardin teaches wherein the unsecure network is the Internet (Figure 1 [block 150]; column 3, lines 46-60).

20. Regarding claims 9 and 24, Jardin teaches wherein the origin server is an effective origin server (column 3, line 61-67).

21. Regarding claims 10 and 23, Jardin teaches wherein the client is an effective client (column 3, lines 46-60).

22. Regarding claims 11 and 25, Ranger teaches wherein the method is performed by a proxy within the given network (Figure 4 [block 64]; column 4, lines 34-47; column 5, lines 41-58).

23. Regarding claims 12 and 26, Ranger teaches wherein the method is performed by a firewall within the given network (Figure 4 [block 64]; column 3, line 66 to column 4, line 21; column 5, lines 41-58).

24. Regarding claims 13 and 27, Ranger teaches a computer-readable medium having a computer program stored thereon for execution by a processor (column 3, lines 41-46).

25. As per claim 14, Jardin teaches a method comprising:

receiving unencrypted data from a client over a secure network in a first hop (column 4, lines 34-43);

26. Jardin does not disclose performing a test relative to the unencrypted data, the test yielding one of at least a first result and a second result.

27. Ranger discloses performing a test relative to the unencrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network. Subsequently if the data did not contain a virus, Trojan horse, or any other malicious code, the unencrypted data would be transferred to a server over a given network in the second hop.

28. Jardin discloses encrypting the unencrypted data into encrypted data (Figure 3 [blocks 336]; column 7, lines 6-19).

29. Both Jardin and Ranger disclose transmitting the encrypted data to a server over an unsecure network. Jardin discuses this in at least figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56, while Ranger offers discussion of this in at least column 4, lines 35-53.

30. Regarding claim 17, Jardin teaches wherein the encrypted data is sent to the origin server over the unsecure network in the second hop within a secure socket layer (SSL) session (column 7, lines 6-19).

31. Regarding claim 18, Ranger teaches wherein the secure network is a carrier network (Figure 4; column 5, line 41 to column 6, line 18).

32. Regarding claim 20, Jardin teaches wherein the client is a thin client (Figure 1 [block 110]; column 3, lines 46-60).

33. Regarding claim 21, Jardin teaches wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, and a wireless phone (Figure 1 [block 110]; column 3, lines 46-60).

34. Regarding claim 22, Jardin teaches wherein the secure network is one of a wired network (Figure 1, column 3, lines 46-60).

35. Jardin and Ranger do not disclose the use of a secure wireless network

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a secure wireless network, since it has been held that it requires only ordinary skill in the art to enable a network to be portable and remove wires to make the network more aesthetically pleasant. See MPEP § 2144.04; see *In re Seid*, 161 F.2d 229, 231, 73 USPQ 431, 433 (CCPA 1947); see *In re Lindberg*, 194 F.2d 732, 735, 93 USPQ 23, 26 (CCPA 1952).

37. As per claim 28, Jardin teaches a system comprising:

a client to send encrypted data over an unsecure network in a first hop (Figures 1 [blocks 110, 150], 3 [blocks 310]; column 6, lines 1-13);

a proxy within a secure network to receive the encrypted data and decrypt the encrypted data into decrypted data, the proxy sending the decrypted data over the secure network in a second hop (Figures 1 [block 120], 3 [blocks 330, 340]; column 4, lines 34-47; column 6, line 58 to column 7, line 5; column 7, lines 38-57); and,

an origin server within the secure network to receive the decrypted data (Figure 3 [block 346]; column 7, lines 38-57).

38. Jardin does not disclose wherein the data is transmitted in response to performing a test relative to the decrypted data yielding a particular response.

39. Ranger discusses wherein the data is transmitted in response to performing a test relative to the decrypted data yielding a particular response, wherein the Examiner interprets the response to be the virus free result of a virus check performed on the data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

40. Regarding claim 29, Jardin discloses sending unencrypted data over a secure network in column 4, lines 24-47. Jardin also discloses a proxy within a secure network to receive the unencrypted data, wherein the second proxy encrypts the unencrypted data into encrypted data and sending the encrypted data over an unsecure network in at least figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56.

41. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960). This is particularly important if the test yields a second result, which the Examiner interprets as the data having malicious code, because it would allow the malicious code to be quarantined thereby making it unable to infect other computers or applications.

42. Regarding claim 30, Jardin discloses a client to send encrypted data over an unsecure network in at least Figures 1 [blocks 150], 3 [block 310], column 6, lines 1-13. Jardin also discusses the use of a proxy to receive encrypted data, decrypt the encrypted data, and transmitting the encrypted data over the unsecure network.

43. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960). This is particularly important if the test yields a second result, which the Examiner interprets as the data having malicious code, because it would allow the malicious code to be quarantined thereby making it unable to infect other computers or applications.

44. As per claim 31, Jardin teaches a system comprising:

a client to send unencrypted data over a secure network in a first hop (column 4, lines 34-43);

a proxy within the secure network to receive the unencrypted data, the proxy encrypting the unencrypted data into encrypted data and sending the encrypted data over an unsecure network in a second hop (Figures 1 [block 120], 3 [blocks 330, 336, 340]; column 4, lines 34-47; column 6, line 58 to column 7, line 19); and,

an origin server to receive the encrypted data (Figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56).

45. Jardin does not disclose wherein the data is transmitted in response to performing a test relative to the unencrypted data yielding a particular response.

46. Ranger discusses wherein the data is transmitted in response to performing a test relative to the unencrypted data yielding a particular response, wherein the Examiner interprets the response to be the virus free result of a virus check performed on the data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

47. Regarding claim 32, Jardin discloses a proxy within a secure network to receive encrypted data encrypted data and decrypt the encrypted data into decrypted data and sending the decrypted data over the secure network to be received by a server in at least figures 1, block 120, 3, blocks 340 and 346, as well as column 4, lines 34-47 and column 7, lines 38-57.

48. It would have been obvious to one of ordinary skill in the art to include a second proxy and a second server, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

49. As per claim 33, Jardin teaches a proxy comprising:

one or more communication components enabling the proxy to communicate over a first network and a second network (Figure 1 [blocks 118, 128]; column 3, lines 46-60);

a computer-readable medium having a computer program stored thereon for execution by the processor to receive data that is originally encrypted or unencrypted from a client over the first network in a first hop and decrypt the data where the data was originally encrypted, sending the data unencrypted to an origin server over the second network in a second hop where the data was originally encrypted, and sending the data unencrypted or encrypted to the origin server over the second network in a second hop where the data was originally unencrypted (Figures 1 [blocks 150], 3 [blocks 310, 330, 336, 346], column 4, lines 34-43; column 6, lines 1-13, column 6, line 58 to column 7, line 19; column 7, lines 53-56). Typical Internet devices described in Jardin comprise processors.

50. Jardin does not disclose performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result.

51. Ranger discloses performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

52. Regarding claim 34, Jardin teaches wherein the first network is a secure network (column 4, lines 24-47).

53. Regarding claim 35, Jardin teaches wherein the second network is an unsecure network, such that sending the data to the origin server over the second network in the second hop comprises first encrypting the data (Figure 3 [block 336, 338]; column 7, liens 6-38).

54. Regarding claim 36, Jardin teaches wherein the second network is a secure network (column 7, lines 6-19).

Conclusion

55. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

56. The following patents are cited to further show the state of the art with respect to secure transmissions, such as:

United States Patent No. 6,253,326 to Lincke et al., which is cited to show a system for secure communications.

United States Patent No. 6,640,302 to Subramaniam et al., which is cited to show secure intranet access.

United States Patent No. 6,721,424 to Radatti, which is cited to show hostage system for intercepting encrypted hostile data.

United States Patent No. 6,397,335 to Franczek et al., which is cited to show computer virus screening methods.

57. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

58. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

59. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100